METHODS AND APPARATUS FOR SECURE COLLECTION AND DISPLAY OF USER INTERFACE INFORMATION IN A PRE-BOOT ENVIRONMENT

ABSTRACT

[0073] Methods and apparatus for secure collection and display of user interface information in a pre-boot environment are disclosed. A disclosed system executes trusted software under a secure mode of a processor. In the secure mode, the processor may directly access an area of memory that normally cannot be accessed. One or more software routines, device drivers, digital certificates, hash codes, encryption keys, and/or any other data may be stored in the secure area of memory. Software routines and device drivers stored in the secure area of memory and/or certified by data in the secure area of memory may be "trusted." Preferably, trusted software routines and/or device drivers are digitally signed by a trusted source (e.g., Microsoft). In addition to trusted interface objects, the pre-boot environment may include non-trusted interface objects. These non-trusted interface objects may use third party software routines and/or device drivers. Accordingly, both trusted and non-trusted interface objects may be used in the same pre-boot interface.